STATEMENT

OF

LOUIS F. ROSENTHAL

EXECUTIVE VICE PRESIDENT

LASALLE BANK CORPORATION

ON BEHALF OF

BITS AND THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,

INTERGOVERNMENTAL RELATIONS AND THE CENSUS

UNITED STATES CONGRESS

HEARING ON

INFORMATION SECURITY—

VULNERABILITY MANAGEMENT STRATEGIES AND TECHNOLOGY

JUNE 2, 2004

TESTIMONY OF LOUIS F. ROSENTHAL
EXECUTIVE VICE PRESIDENT, LASALLE BANK CORPORATION

Introduction

Thank you, Chairman Putnam and Ranking Member Wm. Lacy Clay, for the opportunity to testify before the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census about the ways the financial services sector is addressing information security and our strategies and technologies for managing vulnerabilities.

I am Louis F. Rosenthal, executive vice president, LaSalle Bank Corporation. I am pleased to appear before you today on behalf of The Financial Services Roundtable (The Roundtable) and BITS. LaSalle is one of the largest banks in the Midwest and second largest in Chicago, serving individuals, small businesses, middle market companies and institutions. LaSalle Bank Corporation is a subsidiary of Netherlands-based ABN AMRO Bank N.V., one of the world's largest banks with total assets of EUR 639.9 billion (781.7 billion USD) and a presence in more than 3,000 locations in over 60 countries.

I am also a member of the Executive Committee of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the US. BITS is the sister organization to The Financial Services Roundtable. BITS members hold about $9 trillion of the nation's total managed financial assets of about $18 trillion. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. BITS is not a lobbying organization. Our work in crisis management coordination, cyber security, critical infrastructure protection and fraud is shared not only among our member companies but throughout the financial services sector. BITS works with other critical infrastructure sectors, government organizations, technology providers and third-party service providers to accomplish its goals.

Information security is a complex challenge. Among industry sectors, the financial sector is particularly aware of the challenge, in part because customer trust is so vital to the stability of

financial services and the strength of the nation's economy. At the same time, we are a favorite target of criminals operating in cyberspace and of terrorists, as was made clear on 9/11.

Through BITS, our industry has been at the forefront of advancing security in financial services. However, all interested parties in the private and public sectors must work together if we are to address these issues sufficiently. I would like to recognize and thank Chairman Putnam and subcommittee staff for their outstanding work on public-private information security partnerships, particularly for leading the Corporate Information Security Working Group. You understand, as we do, that the risks for national security and economic soundness cannot be underestimated. Neither can the importance of our working together to address them.

Financial Industry Perspective

Ensuring software security is enormously costly for the financial services industry. In December of 2003, BITS surveyed its members on the cost of addressing software vulnerabilities, including managing software patches. We found that:

- Software vulnerabilities are approaching a cost of $1 billion annually to the financial services industry.
- BITS and Roundtable member companies pay an estimated $400 million annually to deal with software security and patch management issues.
- Just managing patches—which is only a fraction of what we do to deal with vulnerabilities— costs BITS and Roundtable members an estimated $55 million annually and costs the industry an estimated $110 million annually.

The inadequate levels of security within the software our industry purchases, coupled with current inefficient software-patching processes, cause our industry to spend millions of dollars that could be better used for other purposes such as enhancing security and business-continuity practices and offering products and services at lower cost to our customers.

This is an alarming issue and critical to protecting the nation's infrastructure. As I speak, hackers are writing code to compromise systems. Viruses are epidemic. Hackers are closing the window between the discovery of a flaw and the release of a new virus. They are employing the tactics of spammers to rapidly spread their destructive code globally. We are increasingly concerned that a coordinated cyber attack of some kind could impact communications, Supervisory Control and Data Acquisition (SCADA) systems, or first responder systems and put all of us at terrible risk.

The problems are worsening. Attacks on all types of businesses are escalating. Financial services companies are a particularly attractive target. The Deloitte Global Security Survey 2004 finds that the majority of global financial institutions have seen an attack on their IT systems within the last year, and that many of those breaches resulted in financial loss. Eighty-three percent of respondents reported their systems had been compromised in 2003, versus 39 percent in 2002.

As you know, financial institutions are heavily regulated and actively supervised by the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. With the substantial risks of software security, regulators are stepping up their oversight even further. Our industry is working consistently and diligently to comply with new regulations. However, regardless of how well institutions respond to regulations, we simply cannot address these problems alone. Our partners in the software industry must also do their fair share to ensure the soundness of our nation's critical infrastructure.

Financial Industry Efforts

Consumer trust is essential to the success of all US financial institutions. Central to BITS' mission is sustaining that trust. BITS has been advancing security in the financial services industry since its inception in 1996. The BITS Security and Risk Assessment (SRA) Working Group, for example, represents more than 70 of the nation's largest banking, securities and insurance organizations.

The SRA has evolved to meet the increasingly important information security issues of our members and the industry. In October of last year, BITS increased its focus on flawed software with a Software Security and Patch Management initiative to respond to increasing security risks and headline-sweeping viruses. BITS' goal with this work is to mitigate security risks to financial services consumers and the financial services infrastructure, ease the burden of patch management caused by vendor practices, and help member companies comply with regulatory requirements.

BITS is working to encourage a higher "duty of care" by software vendors that sell to critical infrastructure industry companies, to promote compliance with security requirements before software products are released, and to make the patch-management process more secure and efficient and less costly to organizations.

Also in October of 2003, BITS began forging partnerships with the vendors of software most commonly used in our industry. In February of 2004, BITS and The Financial Services Roundtable held a Cybersecurity CEO Summit. The event launched BITS and Roundtable efforts to promote CEO-to-CEO dialogue on software security issues. More than 80 executives from financial services, other critical infrastructure industries, software companies, and government discussed software vulnerabilities and identified solutions. A "toolkit" with software security business requirements, sample procurement language, and talking points for discussing security issues with IT vendors was distributed to 400 BITS and Roundtable member company executives. A theme of the event was the importance of collaborating with other critical infrastructure industries and government. Since the Summit we have worked with all the associations representing the financial services industry, The Business Roundtable and some sector-specific associations.

In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and the Roundtable support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products. We are also seeking protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase. Additionally, as part of the policy, BITS and the Roundtable are encouraging regulatory agencies to explore supervisory tools to ensure critical third-party service providers and software vendors deliver safe and sound products and services to the financial services industry.

Today, we are working with software companies to create solutions acceptable to all parties. We have provided these companies with a series of business requirements that BITS members agree are critical to the soundness of systems used in the financial services industry.

BITS is also working with other critical infrastructure industries and industry associations to help motivate a larger user movement. Most recently, BITS' consultation and collaboration with The Business Roundtable resulted in that organization's widely publicized response to the state of software security. The Business Roundtable called on software producers and end users to work together to build a more unified defense against the increasing number and growing cost of cyber attacks.

The BITS Product Certification Program is another important part of our work to address software security. The BITS Product Certification Program is a testing capability that provides security criteria against which software can be tested. A number of software companies are considering testing. The criteria are also used by financial institutions in their procurement processes.

This summer, BITS will publish best practices for patch management from the user's perspective. As I mentioned earlier, patch management and implementation alone can cost one financial institution millions of dollars annually. Cost aside, it is critical for patches to be prioritized, and implemented as quickly as possible, given the speed with which viruses are targeting new vulnerabilities.

We urge the Committee to consider all aspects of critical infrastructure—the software and operating systems, the critical infrastructure industries, and the practices of firms, industries and the government—in addressing software security and vulnerability management.

Recommendations

We have developed six key recommendations for the Committee to consider:

1. **Encourage providers of software to the financial services industry to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure.** Software providers need to exhibit and be held to a "higher duty of care" to satisfy their own critical infrastructure responsibilities.

2. **Support measures that make producers of software more accountable for the quality of their products.**
    a. Ensure their products are designed to include security as part of the development process.
    b. Test that their products meet quality standards and that financial services security requirements are met <u>before</u> products are sold.
    c. Develop patch-management processes that minimize costs, complexity, downtime, and risk to user organizations. Software vendors should identify vulnerabilities as soon as possible and ensure that the patch is thoroughly tested.
    d. Continue patch support for older, but still viable, versions of software.

3. **Provide incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation**

of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products.

4. **Provide protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.**

5. **Encourage collaboration and coordination among other critical infrastructure sectors and government agencies to mitigate software security risks.**

6. **Encourage regulatory agencies to review software vendors—similar to what the regulators currently do in examining third-party service providers—so that software vendors deliver safe and sound products to the financial services industry.**

It is important for the Subcommittee to recognize the dependence of all critical infrastructures on software operating systems and the Internet. A clear understanding of the role of software operating systems and their "higher duty of care," particularly when serving the nation's critical infrastructures, needs to be explored. Further, the Subcommittee should recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements. Other industries do not have the same level of regulatory oversight, liability, or business incentives. However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.

On behalf of LaSalle Bank Corporation, BITS, and The Financial Services Roundtable, thank you for the opportunity to testify before you today. I will now answer any questions.